BOBBY JINDAL
GOVERNOR

ANGELE DAVIS
COMMISSIONER OF ADMINISTRATION

State of Louisiana

Division of Administration
OIT Enterprise Security Office

MONTHLY SECURITY TIPS October 2008

Security Patches & Updates – Patch It to Protect It

Understanding Patches

What are patches?

Similar to the way fabric patches are used to repair holes in clothing, software patches repair holes in software programs. Patches are updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch.

Updates to your operating system often close serious security gaps. It is important to install a patch as soon as possible to protect your computer from attackers who would take advantage of vulnerabilities.

How do you find out what patches you need to install?

Each computer runs on a specific operating system (OS) that houses the vital components that allow your computer to work. The three most well-known operating systems are Windows XP/Vista, Macintosh OS X and Linux. In order to keep step with the bad guys, these OS manufacturers issue regular updates (or "patches") that fix specific problems or vulnerabilities in the OS.

These updates are primarily "pushed" to the computer user, meaning the computer automatically receives and downloads those fixes. For home users it is recommended that this "Automatic Updates" option be utilized.

Instead of automatically downloading patches, you can also configure your OS to send an alert when patches become available and then you can choose when to install them. Within an agency or business network, the IT staff will usually push out updates to each computer after business hours.

Managing updates for hundreds of machines can be a daunting challenge. To accomplish this task an IT staff will likely use a "Patch Management" tool such as Ecora Patch Manager, Novell ZENworks, PatchQuest, or Windows Server Update Services (WSUS).

Michael Gusky, Chief Information Security Officer
Tel: (225) 219-9475 • Cell: (225) 247-6588 • Mike.Gusky@la.gov

Patches can also be downloaded at any time from the OS vendor's website. Here are links to the update pages for the major OS vendors:

- http://update.microsoft.com/windowsupdate
- http://www.apple.com/support/leopard/
- http://www.linuxhq.com/

What are the risks of having un-patched systems?

Hackers are always looking for new ways to exploit users of older and out-of-date systems. It is estimated that the surival time of an un-patched computer connected to the internet is less than four minutes. They can use un-patched vulnerabilities or problems in these systems to gather personal information, install malicious software (malware) and launch attacks against other machines.

Just like one leak can sink a boat, one un-patched system can sink an entire organization; however by keeping your computer updated and patched you will provide an additional layer of security for your system, and your data.

The information provided in this Monthly Security Tips Newsletter is intended to increase the security awareness of end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the State's overall cyber security posture

Michael Gusky, Chief Information Security Officer
Tel: (225) 219-9475 • Cell: (225) 247-6588 • Mike.Gusky@la.gov